

Sicurezza delle reti IP

Antonio Lioy
<lioy@polito.it>

Politecnico di Torino
Dip. Automatica e Informatica

Reti private

- molte organizzazioni non hanno bisogno che alcuni loro indirizzi siano visibili globalmente (es. display TCP/IP degli aeroporti)
- per evitare di sprecare indirizzi la IANA ha definito delle reti private (RFC-1918):
 - indirizzi non unici a livello mondiale
 - usabili senza chiedere autorizzazione purché si garantisca che siano limitate alla rete interna

Classi per le reti private

- classe A (una sola rete)
rete: 10.x.x.x = 10/8
- classe B (16 reti adiacenti)
reti: 172.16.x.x ... 172.31.x.x = 172.16/12
- classe C (256 reti adiacenti)
reti: 192.168.0.x ... 192.168.255.x = 192.168/16
- anche dette 24 / 20 / 16-bit blocks

Organizzazione di una rete privata

- host pubblici con indirizzo IANA
- host privati con indirizzi privati
- due soluzioni per accedere da host privati a servizi pubblici:
 - application gateway (proxy) sugli host pubblici
 - network address translator (NAT)

Network address translator (NAT)

- traduzione degli indirizzi IP privati in indirizzi pubblici in modo automatico:
 - in modo statico (uno a uno)
 - in modo dinamico (uno per molti)
- svantaggi:
 - limite di prestazioni
 - servizi pubblici richiedono indirizzo fisso
 - problemi con UDP e quando gli indirizzi IP sono usati a livello applicativo (es. FTP)
- vantaggi:
 - non richiede modifica degli applicativi

RFC per NAT

- RFC-2663 "IP Network Address Translator (NAT) terminology and considerations"
- RFC-2766 "Network Address Translation - Protocol Translation (NAT-PT)"
- RFC-2993 "Architectural implications of NAT"
- RFC-3022 "Traditional IP Network Address Translator (traditional NAT)"
- RFC-3027 "Protocol complications with the IP Network Address Translator"

NAT

- **implementazione software:**
 - processo su un dual-homed host
 - es. per Linux, Windows NT/2000/XP
- **implementazione hardware:**
 - nei router

Application gateway (proxy)

- **funzionamento:**
 - riceve richiesta da Hpri
 - inoltra richiesta col proprio IP (pubblico)
 - riceve risposta
 - inoltra risposta a Hpri
- **richiede consapevolezza dell'esistenza del proxy da parte del richiedente**
- **permette di far passare selettivamente solo certi protocolli / richieste / utenti**
- **protocollo di proxy**

Accorgimenti pratici

- **cablaggio separato per la parte pubblica e privata (problemi di routing e netmask)**
- **stessa sottorete per host con stesso destino (o tutti pubblici o tutti privati)**
- **filtri sui router verso le reti pubbliche per non propagare le informazioni circa la rete privata:**
 - pericoloso per la sicurezza
 - malfunzionamento del routing globale
